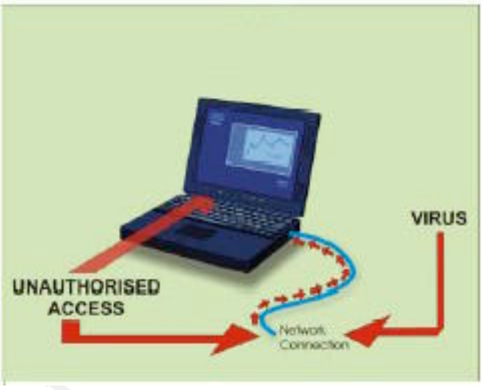
How we automated Basic Security Rules Implementation On Workstations



GIAC Security Essentials Certification
(GSEC)
Practical Assignment
Version 1.4c

Option 2

Submitted by: Jean-Denis BIGNON, December 03, 2004
Location: SANS Conference - London - June 2004

Tables of Contents

Abstract

In this paper, I would like to describe how in my worldwide company,
The workstation‘s security problem has been solved (almost!!)
The fact is that the easiest way to compromise the

-Integrity (Information stored on the workstation may be changed – accidentally or maliciously)
-Privacy (information contained within a workstation, should not be disclosed to or accessible by unauthorized user)
-Availability (the system should not deny access to authorized user)
-Confidentiality (Information may be disclosed inappropriately by:
-unauthorized users gain access to workstation
-authorized users gain access to information that they aren't supposed to see)

of the company's data assets is through its workstations.
While we focus on the critical servers having participated in numerous security reviews, we've found the easiest way of gaining access to critical data, is almost always the humble workstation, due to the lack of security awareness of the owner.

Corporate Security audits and Internal Security reviews (a part of my job) have indicated the effort required by employees to keep their workstation compliant to ITCS Corporate Security guidelines (ITCS300) is very time consuming and has resulted in many cases where security compliance has not been met.
This put Company and its infrastructure in a vulnerable situation.
So, to assist employees in becoming compliant, we have called for an automated download solution.

-The Workstation Security Tool was born.

You asked for it, you got it!

The tool is designed to check the compliance of the security rules described in our Corporate Security Guidelines.

This Security Guidelines describes the **basic** computer security measures that must be followed by all employees of the company; employees of company subsidiaries; contractors, vendors and others authorized by the management to use the company's internal systems.
This document includes two major sections:
-The first summarizes the most critical steps employees must take to protect personal workstations provided by the company and to defend company's systems against harmful code
-The second summarizes employees responsibilities for protecting confidential information and lists security and appropriate usage requirement in a number of other circumstances that employees are likely to encounter.

In my business unit (over 2000 employees) I have some responsibilities:
(IT Security Education - Physical Security (DP Centers) - Internal security reviews

I was chosen by my management to be the interface of the business unit and to lay the groundwork for the tool

What was my role?
(Frankly, it was a modest one)
A) The first step was to enhance the security education
I wrote a security package:
-What are the stakes of the IT Security
-What are the security policies that are relevant to the business unit.
-Focus attention on the corporate security guidelines
I presented the package to my business unit

B) I tested the tool on my workstation (as many others)
-feedback, checkpoint, meetings, confcall's ….
C) Deployment and education on the tool in the business unit
D) To day I'm still the interface and the focal point of problems encountered by users

It'll be wrong to say that anything was done before it
But the Basic security rules were not correctly implemented and it was impossible to check the compliance of all workstations (sampling and manual checks), and a lot of users didn't give a damn about that.

Sure, it's not a miracle tool but thanks to it the compliance is getting better than before and it made the users becoming aware of the importance to protect their workstations.

SAM

I can write about WST without describing its technical environment

What is SAM?

The Standard Asset Manager (SAM) is a worldwide application of my company which resides on the client workstation, and provides user and machine information.
SAM is a key component of my company Workstation Asset Management Tool suite.
It indicates the technology level of each workstations allowing better planning and monitoring of the hardware replacement/software upgrade processes in order for the company to make critical business decisions and to ensure compliance of the workstation to the basic security standards established by ITCS300 through the automated delivery of the Workstation Security Tool (WST).
Finally, all this data is stored on local files that will be transmitted to a central repository, the Workstation Asset Management (WAM) database.

A scan is scheduled every 2 weeks. It reads key hardware information from the local BIOS (e.g. Type-Model-Serial number, speed of the processor, size of the hard disk and memory) and it gathers the software information based on a predefined list of applications specified in the SAM software dictionary. This dictionary contains only applications that are part of the Client for e-business and application in the Standard Software Installer* (SSI).

**SSI: Download and install approved Company's software delivery tool*
Delivers software to employees in easy-to-use installable packages
Is accessible over the intranet
Includes a wide range of business applications standard across company

To comply with Data Privacy rules, SAM can neither scan the content of any document nor the software outside the scope of the agreed software dictionary.

Are users required to install SAM?

The installation and registration of SAM is mandatory.
All Worldwide user with workstation,(Notebook PC or Desktop) including Microsoft Windows users, which are company owned workstations that connect to the
Company. Network
SAM supports all clients for e-business* Microsoft Windows 2000 and XP
For Linux a special SAM is in progress.

**Clients for e-business (C4eb):*
Are applications that are part of the standard company available in SSI
Each Workstation is issued to employee with the C4eb standard software

A primary workstation is a desktop or Notebook PC which is used as an office productivity platform for normal office work (e-mail, web browsing/applications, instant messaging, documentation, etc…), and which are not used for multiple user capabilities (e.g. server functions). While secondary PCs, classrooms PCs, and lab

PCs, and home personal PCs are out of scope of this standard, it is highly desired that all PCs install and run SAM that connect to the company network so that strategic business decisions can be made based on the hardware, software and security in use throughout the corporation.

What does user need to do?

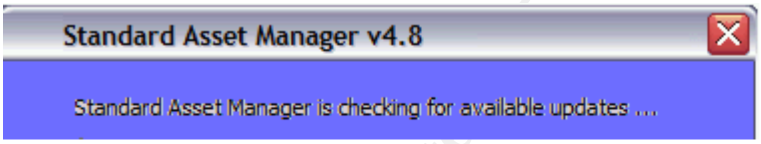
The tool has to be used by all type of users in Pages directory* (regulars, contractors, suppliers, ….) unless there is a valid exemption reason for them not to use the tool.

**Pages directory: Search the company corporate directory with a variety of attributes (internet address, Name, Userid, Job responsibility, Notes address, etc…..)*

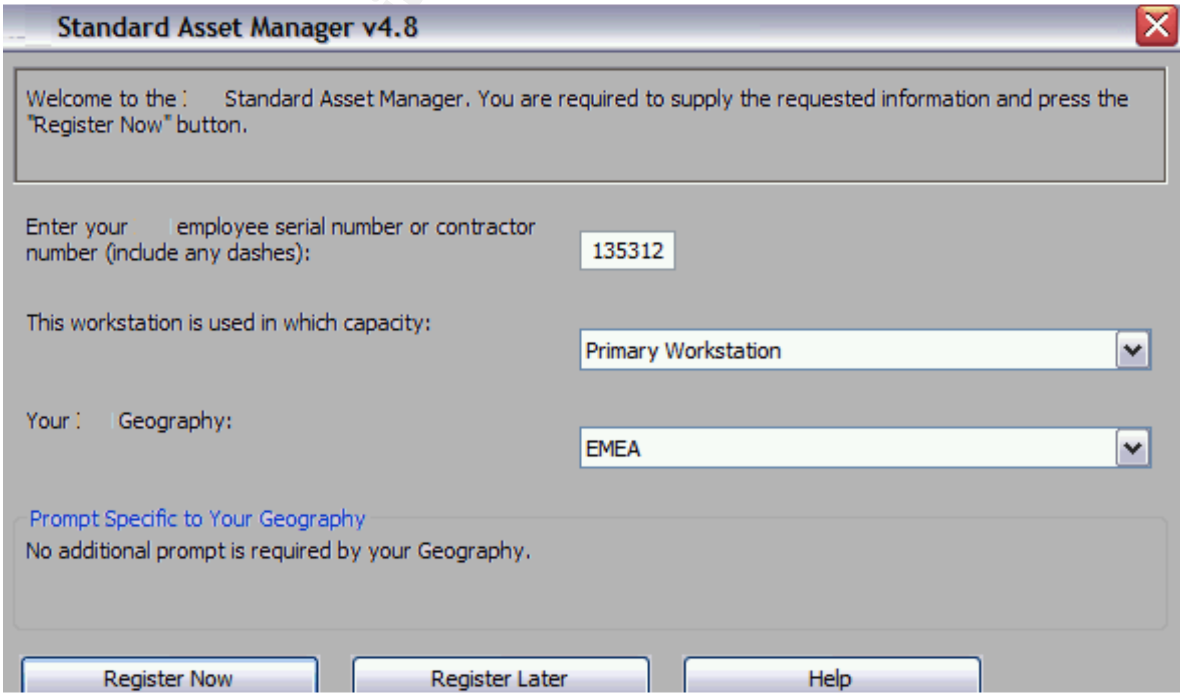
The first time during the registration of SAM he/her will be asked to provide the following information to register his/her workstation in the database

-Employee Serial Number
(the first six digits are obligatory, including letters and/or zeroes)
-Workstation capacity
(Primary, Secondary, Shared, Lab, Classroom Workstation)
-Geography
(Europe, US)

SAM-Screens:



Standard Asset Manager is checking for available updates ....



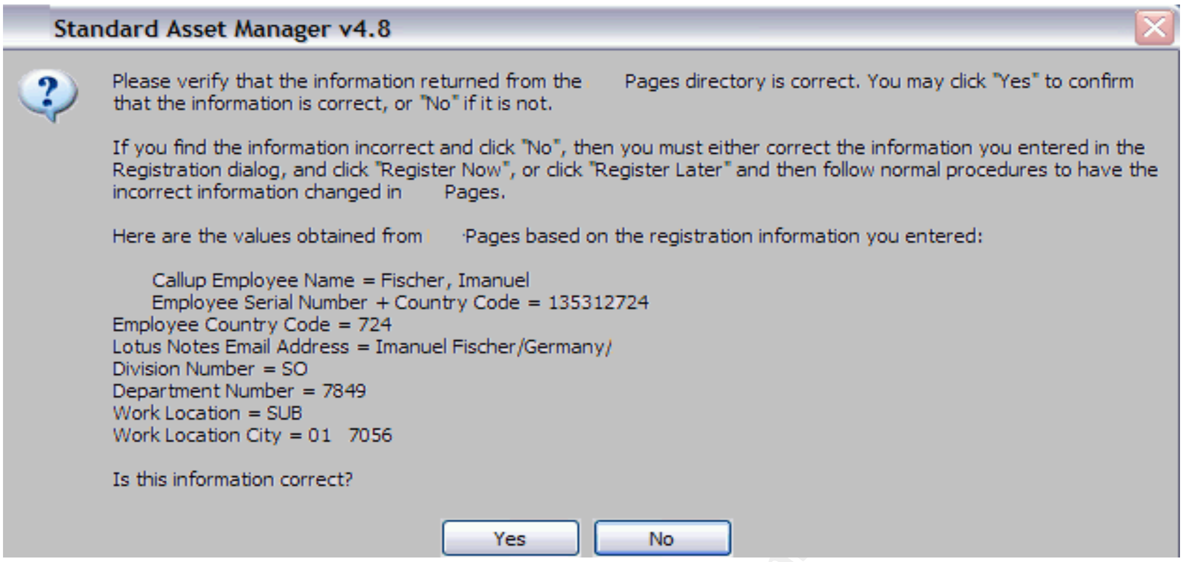
Welcome to the Standard Asset Manager. You are required to supply the requested information and press the "Register Now" button.

Enter your employee serial number or contractor number (include any dashes): 135312

This workstation is used in which capacity: Primary Workstation

Your Geography: EMEA

Prompt Specific to Your Geography
No additional prompt is required by your Geography.



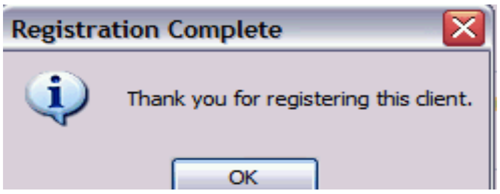
Please verify that the information returned from the Pages directory is correct. You may click "Yes" to confirm that the information is correct, or "No" if it is not.

If you find the information incorrect and click "No", then you must either correct the information you entered in the Registration dialog, and click "Register Now", or click "Register Later" and then follow normal procedures to have the incorrect information changed in Pages.

Here are the values obtained from Pages based on the registration information you entered:

Callup Employee Name = Fischer, Imanuel
Employee Serial Number + Country Code = 135312724
Employee Country Code = 724
Lotus Notes Email Address = Imanuel Fischer/Germany/
Division Number = SO
Department Number = 7849
Work Location = SUB
Work Location City = 01 7056

Is this information correct?



Thank you for registering this client.

How does SAM work?

SAM is activated by filling out the information requested the first time it is launched. The Pages directory is accessed to verify and to enrich the employee data. The scans (hardware and software) occur in the background and are randomly scheduled to run in a “6 hour window” after reboot, not immediately following it.

If a user is not network connected the application goes to sleep and checks for network availability at 5 minute intervals for 30 minutes. If (after 30 minutes) the network is still unavailable the application prompts the user to connect to the network or click ‘cancel’

The average time to run on a client machine is a minute or less. During that time, it will not freeze the workstation and the user can perform other tasks. The storage space required by SAM is about 2.5 MB. This should not pose a storage problem on any PC.

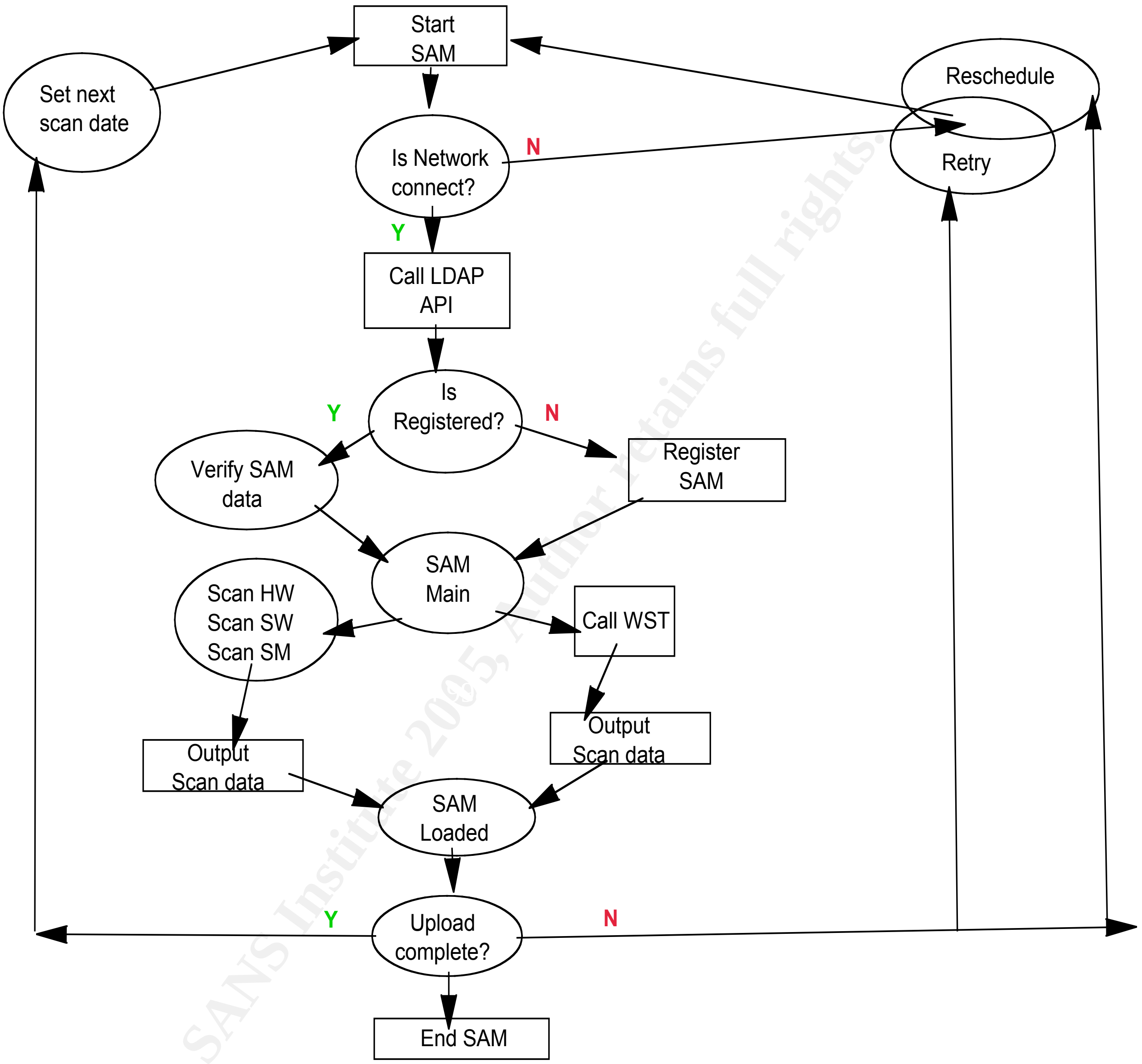


Fig-A: SAM Architecture Application Diagram

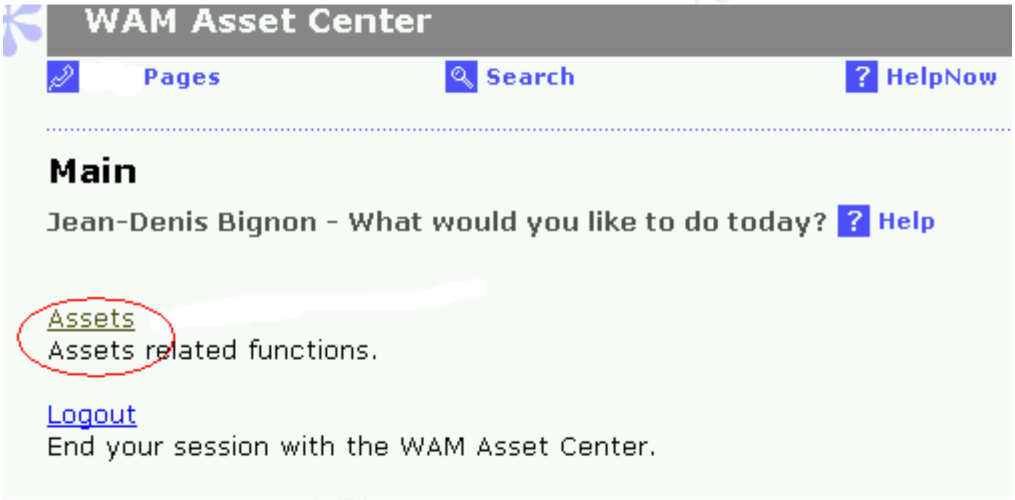
WAM Asset Center (WAC)

The WAM Asset Center (WAC) is a web based tool which is part of the Workstation Asset Management Tool (WAM)
This tool:

- Provides an easy to use view of workstation assets.
- Allows an individual to view ownership, usership , software , security compliance of his/her workstation and other machine specific information.
- Allows managers to view employee's machine ownership, usership, software, security compliance workstation and other machine specific information.

The WAM Asset Center utility catalogs only software that the company tracks on user system which includes Internet –based P2P applications.
This information is gathered when the SAM Tool is installed.
An intranet username and password is required to gain access.

WAM-Screens:

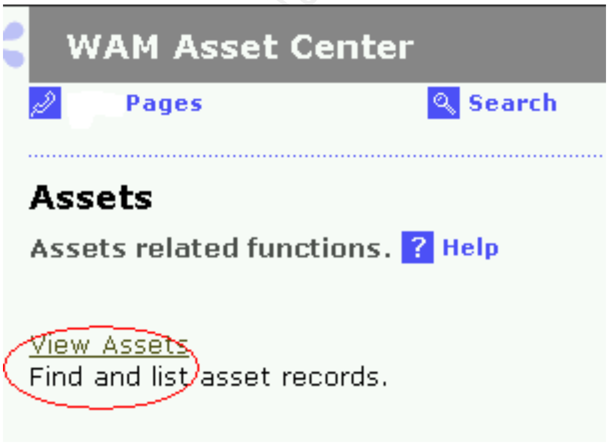


Main

Jean-Denis Bignon - What would you like to do today?

Assets
Assets related functions.

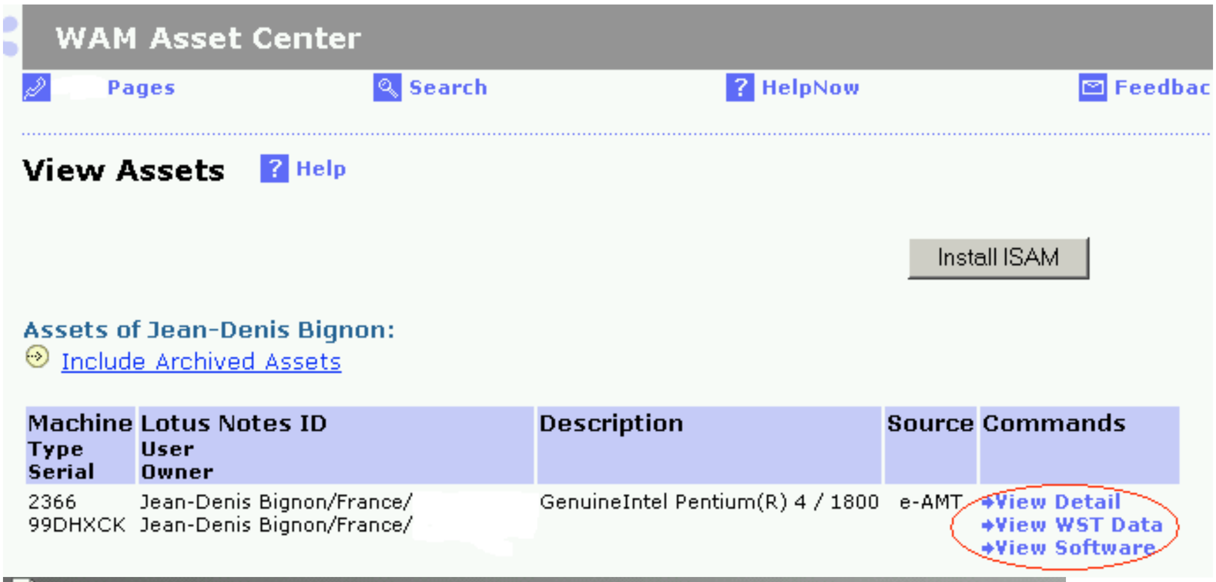
Logout
End your session with the WAM Asset Center.



Assets

Assets related functions.

View Assets
Find and list asset records.

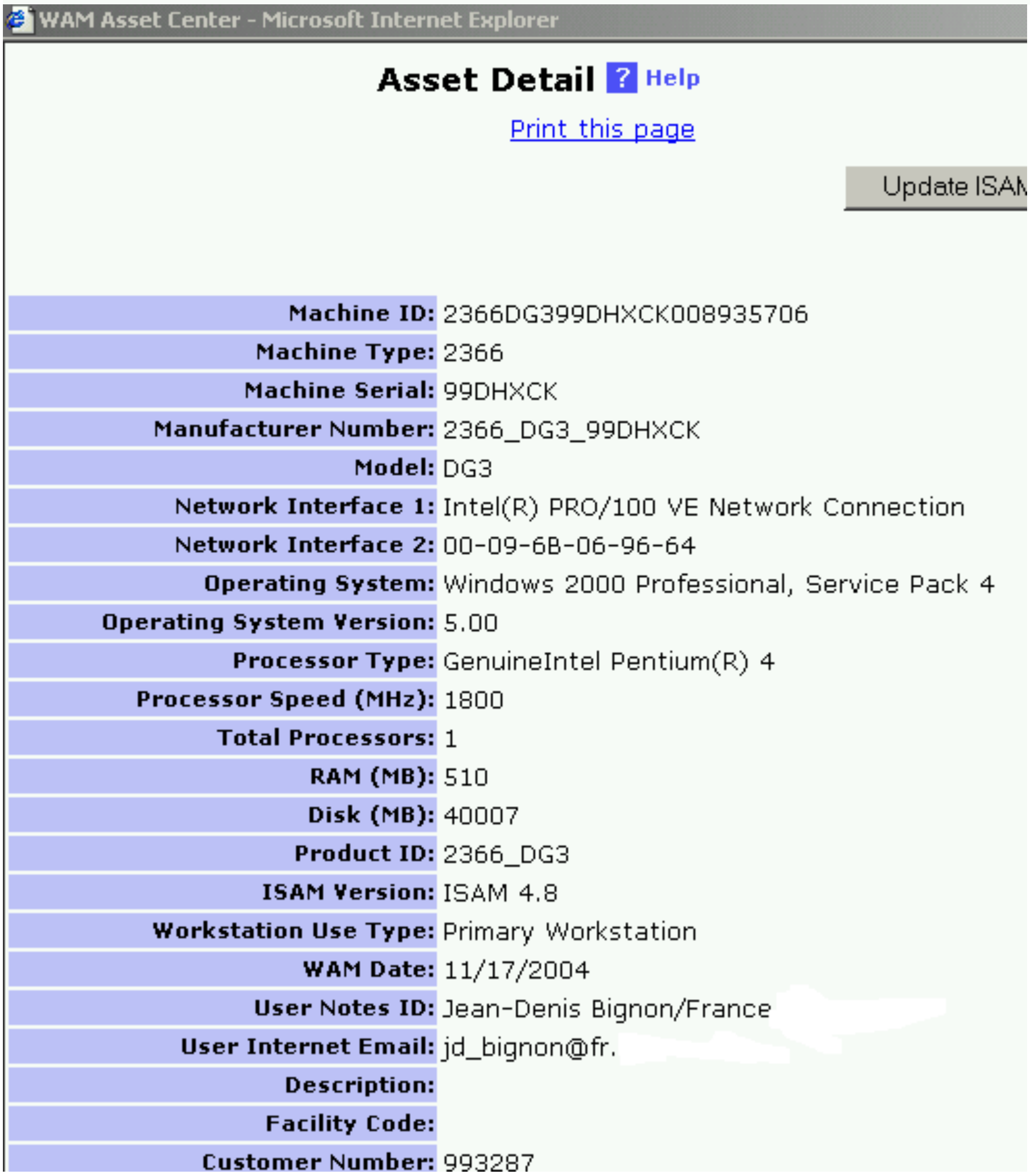


View Assets

Assets of Jean-Denis Bignon:

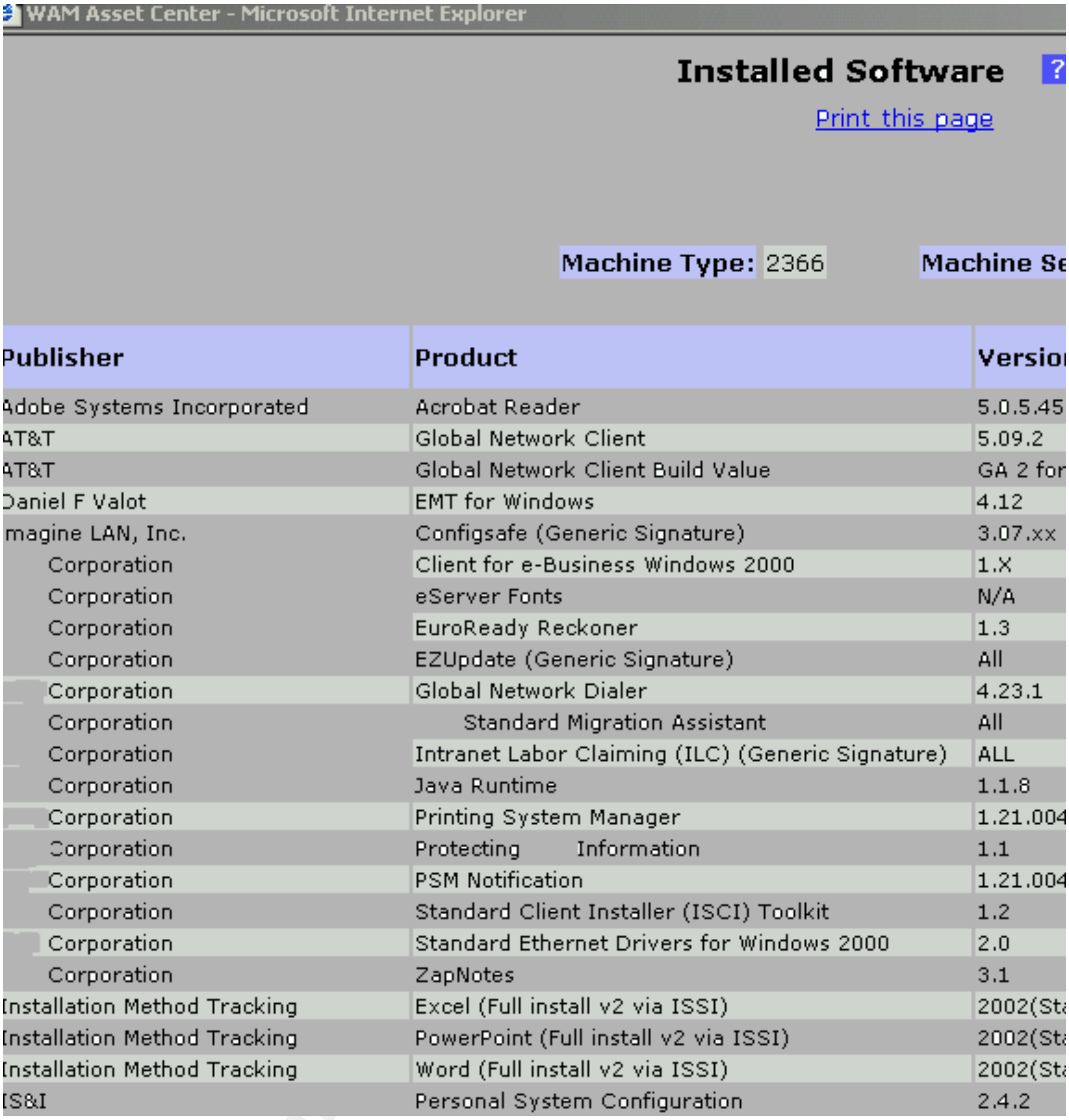
Include Archived Assets

Machine Type Serial	Lotus Notes ID User Owner	Description	Source	Commands
2366 99DHXCK	Jean-Denis Bignon/France/[redacted] Jean-Denis Bignon/France/	GenuineIntel Pentium(R) 4 / 1800	e-AMT	➜View Detail ➜View WST Data ➜View Software



Asset Detail

Machine ID:	2366DG399DHXCK008935706
Machine Type:	2366
Machine Serial:	99DHXCK
Manufacturer Number:	2366_DG3_99DHXCK
Model:	DG3
Network Interface 1:	Intel(R) PRO/100 VE Network Connection
Network Interface 2:	00-09-6B-06-96-64
Operating System:	Windows 2000 Professional, Service Pack 4
Operating System Version:	5.00
Processor Type:	GenuineIntel Pentium(R) 4
Processor Speed (MHz):	1800
Total Processors:	1
RAM (MB):	510
Disk (MB):	40007
Product ID:	2366_DG3
ISAM Version:	ISAM 4.8
Workstation Use Type:	Primary Workstation
WAM Date:	11/17/2004
User Notes ID:	Jean-Denis Bignon/France[redacted]
User Internet Email:	jd_bignon@fr.[redacted]
Description:	
Facility Code:	
Customer Number:	993287



Installed Software

Machine Type: 2366 Machine Se

Publisher	Product	Versio
Adobe Systems Incorporated	Acrobat Reader	5.0.5.45
AT&T	Global Network Client	5.09.2
AT&T	Global Network Client Build Value	GA 2 for
Daniel F Valot	EMT for Windows	4.12
magine LAN, Inc.	Configsafe (Generic Signature)	3.07.xx
Corporation	Client for e-Business Windows 2000	1.X
Corporation	eServer Fonts	N/A
Corporation	EuroReady Reckoner	1.3
Corporation	EZUpdate (Generic Signature)	All
Corporation	Global Network Dialer	4.23.1
Corporation	Standard Migration Assistant	All
Corporation	Intranet Labor Claiming (ILC) (Generic Signature)	ALL
Corporation	Java Runtime	1.1.8
Corporation	Printing System Manager	1.21.004
Corporation	Protecting Information	1.1
Corporation	PSM Notification	1.21.004
Corporation	Standard Client Installer (ISCI) Toolkit	1.2
Corporation	Standard Ethernet Drivers for Windows 2000	2.0
Corporation	ZapNotes	3.1
Installation Method Tracking	Excel (Full install v2 via ISSI)	2002(Sta
Installation Method Tracking	PowerPoint (Full install v2 via ISSI)	2002(Sta
Installation Method Tracking	Word (Full install v2 via ISSI)	2002(Sta
IS&I	Personal System Configuration	2.4.2

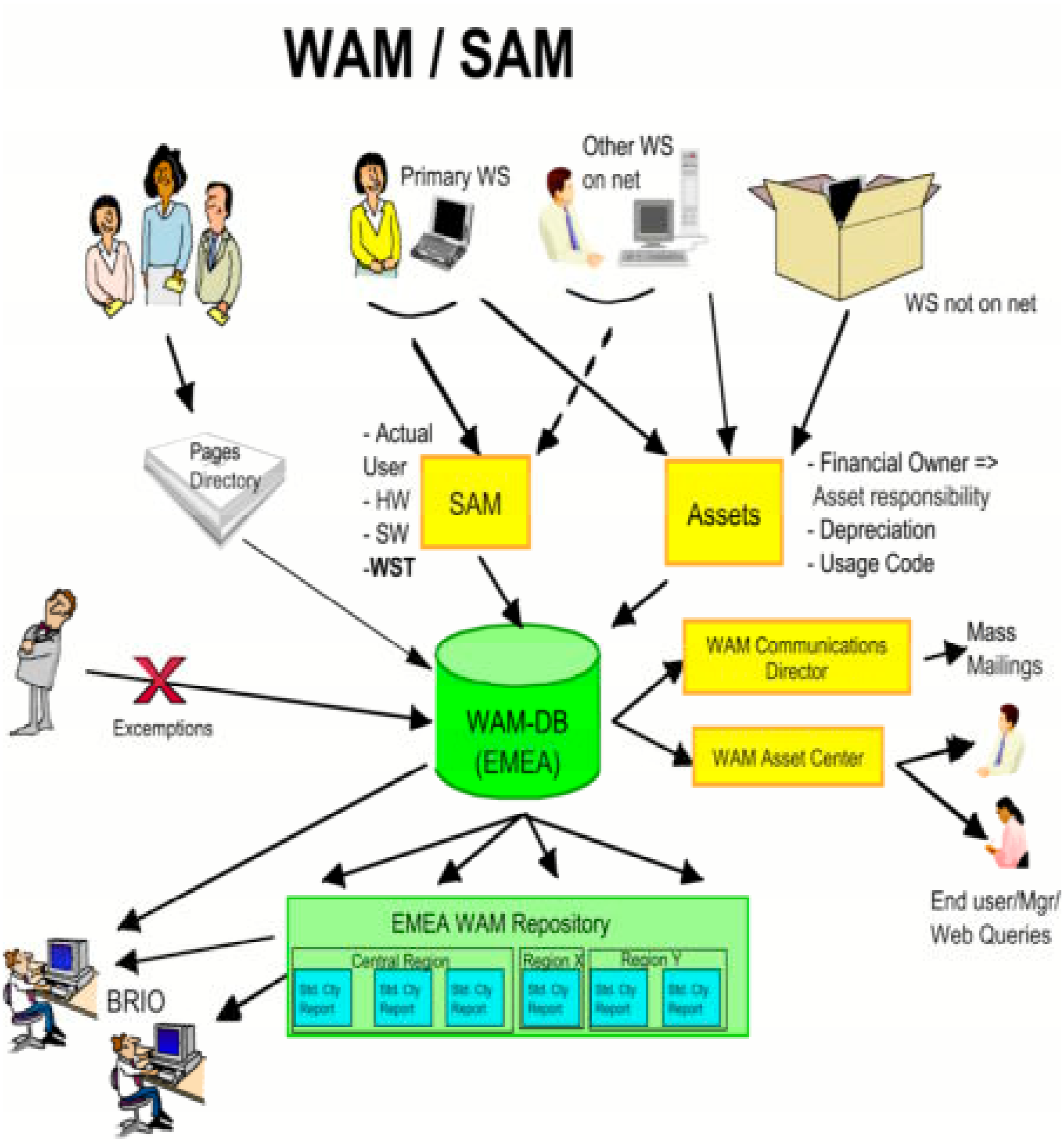


Fig-B: WAM / SAM Infrastructure diagram

WST

To assist employees in becoming compliant, the Workstation Security Tool (WST) is provided to systems running SAM utility.

The Workstation Security Tool checks the IT Security requirements detailed in ITCS300.
The Tool (WST) is a diagnostic PC tool designed to check for employee compliance with the workstation security requirements in the Security and Use Standards for Company Employees.

The tool runs in the background of employee' workstations via the Standard Asset Manager (SAM) every 15 days, and provides employees a report detailing their level of compliance, along with instructions for securing their workstations.

The tool is distributed automatically through SAM to all workstations running Windows 2000 or Windows XP listed as a primary, secondary or shared workstation in the worldwide asset management database.
Following the initial deployment, business units are responsible for ensuring that their employees are registered with SAM and using the tool.

A detailed security report is created on employee's workstations to show their level of compliance or non-compliance. The report indicates which checks caused the workstation to be compliant (green text) or non-compliant (red text).
Instructions on how to fix areas non-compliance are included, along with pointers to additional help. For security measures marked with a yellow question mark it is the employee's responsibility to check the item and ensure it complies with security guidelines.

The results of the security scan are collected and stored in the Workstation Asset Management (WAM) database which can be accessed via the WAM Asset Center.
Data from the results are compiled for use by the business unit security team and management teams.

Basic Security Rules checked by WST

1. **Has a power-on password been set?**
   - ➢ *What is required?*

•Activate power-on password on all workstations

- ➢ *Why is required?*

•To prevent unauthorized access to confidential data on workstations

2. **Has a hard disk password been set?**
   - ➢ *What is required?*

•Activate hard disk password on all Notebooks PC's

- ➢ *Why is required?*

•To prevent unauthorized access to confidential data on Notebook PC hard disk

3. **Is a screen saver active, password protected and set to be activated in less than 30 minutes?**
   - ➢ *What is required?*

•Enable automatic screen lookup after 30 minutes of inactivity

- ➢ *Why is required?*

•To prevent unauthorized access to confidential data on workstations

4. **Is the latest version of Norton Antivirus running, with at least a weekly Live-Update of virus definition files?**
   - ➢ *What is required?*

• Have the latest version of Norton Anti Virus installed and active on all workstations

- ➢ *Why is required?*

• To prevent virus infections which could disrupt workstation, server and network availability as well as destroy data.

5. **Is an approved and the latest version of client firewall installed and running?**
   - ➢ *What is required?*

• Have the latest version and approved personal firewall installed and active on all windows workstations, when connecting to an ISP, customer or vendor network or wireless LANs.

- ➢ *Why is required?*

.To prevent unauthorized access to confidential data on workstations by blocking inbound access to unauthorized traffic.

6. **Have local Notes databases (mail, archive, My Attachments repositories) been encrypted and what is the encryption status of other local databases?**
   - ➢ *What is required?*

• Encrypt all replicas of Lotus Notes databases which contain confidential information

- ➢ Why is required?

• To prevent unauthorized access to confidential data contained in Lotus Notes

7. **Is the Microsoft Windows file sharing feature (if enabled) protected with a user ID or password?**
   - ➢ *What is required?*
- Do not allow any form of unauthenticated access on your network connected workstation
   - ➢ *Why is required?*
- To prevent unauthorized access to confidential data in workstation shared drives or folders

8. **Has the Microsoft Windows Account password (Windows login) been set properly?**
   - ➢ *What is required?*
- Do not allow Microsoft Windows operating system userids to be created on the workstation without password. Password must follow Company password rules
   - ➢ *Why is required?*
- To prevent unauthorized access to confidential data

Check output of WST

For each 'Performed Check' of these Items, an icon will represent the compliance status of them:

✓	WST was able to perform the check and the system **IS** compliant (No action is required). Congratulations
?	WST was **NOT** able to verify compliance **YOU** must verify compliance with this item
X	WST was able to perform the check and the system is **NOT** compliant. **You must take action to resolve this issue!** Click on each 'Performed Check' link for more information about that check, including how to correct this issue

Shortly after the tool runs on the workstations, the employees will receive a follow up e-mail pointing them to their results. The report will indicate those areas with which they are in compliance and those they are not – along with detailed instructions for making necessary adjustments.
Results of the first scan will be sent to employees only.
Subsequent scans will generate a report to managers detailing the compliance of their teams.

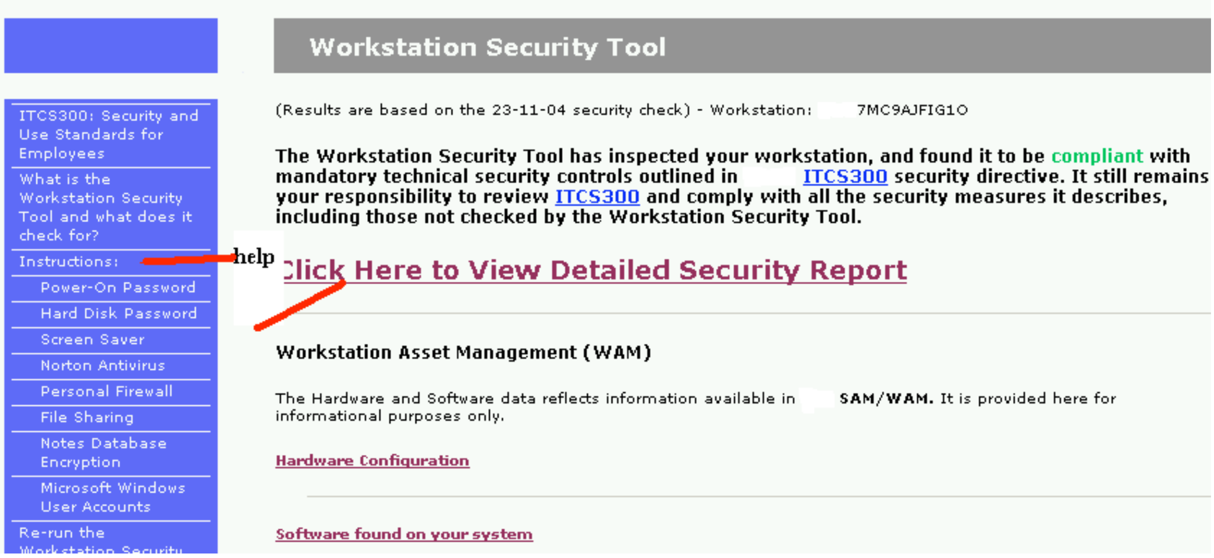
The Workstation Security Tool is looking for the specific security attributes listed above and reports on compliance or non-compliance only.
WST does not examine any personal data or activity performed on the workstation.

The WST Report

The Local Security Report is created on the workstations showing areas of compliance and non-compliance. This report indicates which checks caused the workstation to be compliant or not.
The report can be accessed through the menu

For all employees

Start > Programs > Workstation Security Tool > Last report


ITCS300: Security and Use Standards for Employees
What is the Workstation Security Tool and what does it check for?
Instructions:
Power-On Password
Hard Disk Password
Screen Saver
Norton Antivirus
Personal Firewall
File Sharing
Notes Database Encryption
Microsoft Windows User Accounts
Re-run the Workstation Security
help

Workstation Security Tool

(Results are based on the 23-11-04 security check) - Workstation: 7MC9AJFIG1O

The Workstation Security Tool has inspected your workstation, and found it to be compliant with mandatory technical security controls outlined in ITCS300 security directive. It still remains your responsibility to review ITCS300 and comply with all the security measures it describes, including those not checked by the Workstation Security Tool.

Click Here to View Detailed Security Report

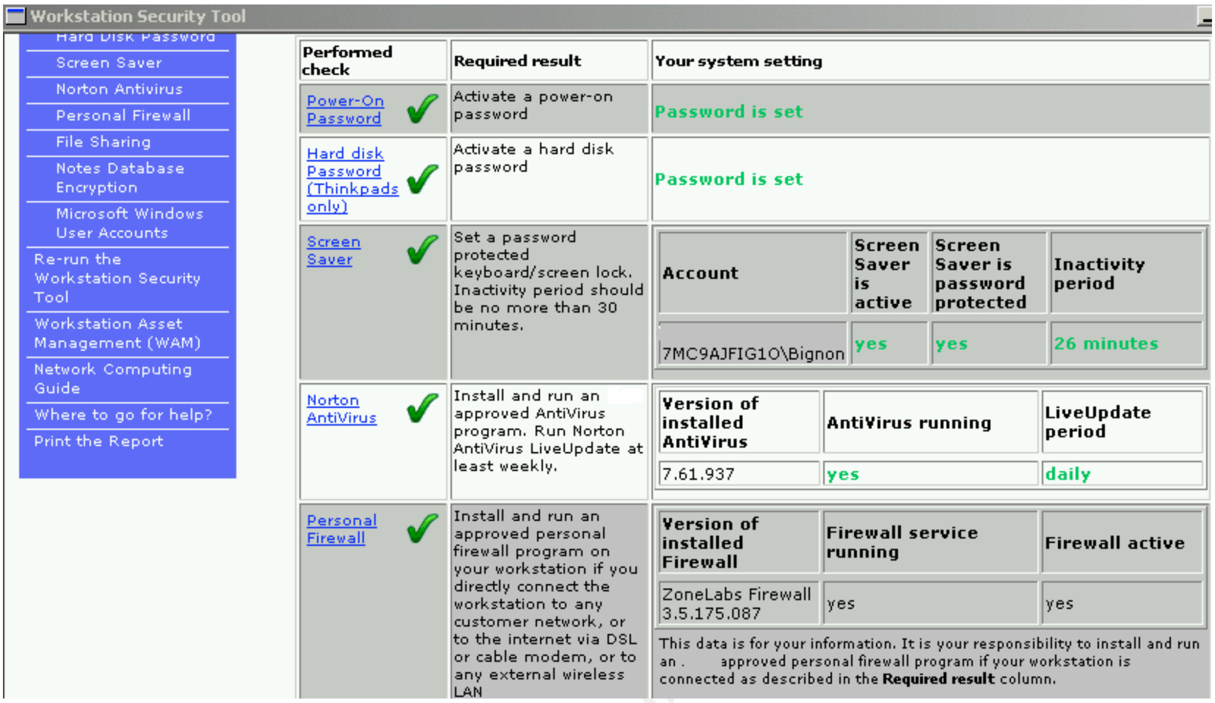
Workstation Asset Management (WAM)

The Hardware and Software data reflects information available in **SAM/WAM.** It is provided here for informational purposes only.

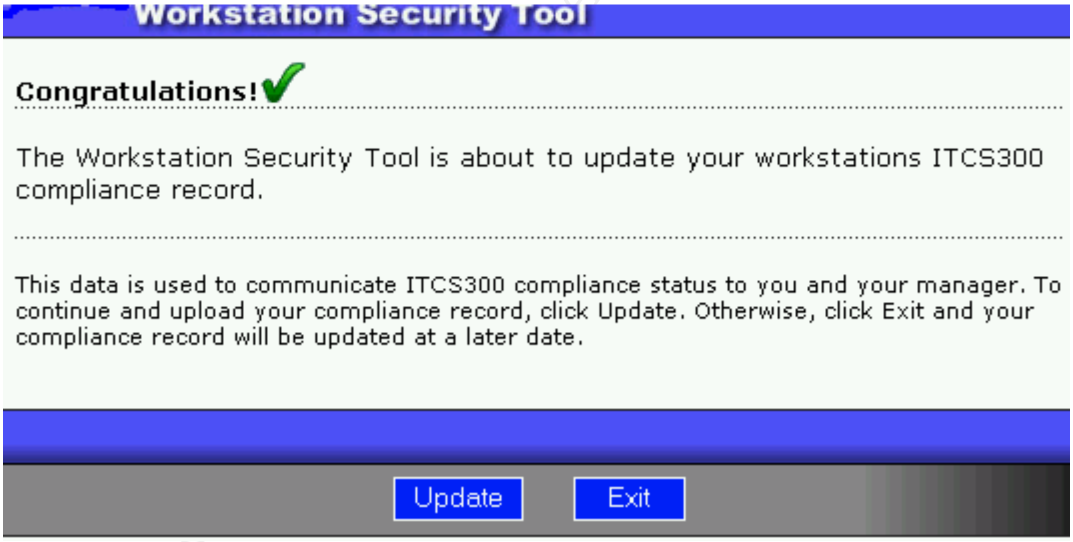
Hardware Configuration

Software found on your system

Example of Compliant Workstation:


Workstation Security Tool
Hard Disk Password
Screen Saver
Norton Antivirus
Personal Firewall
File Sharing
Notes Database Encryption
Microsoft Windows User Accounts
Re-run the Workstation Security Tool
Workstation Asset Management (WAM)
Network Computing Guide
Where to go for help?
Print the Report

Performed check	Required result	Your system setting
Power-On Password ✓	Activate a power-on password	Password is set
Hard disk Password (Thinkpads only) ✓	Activate a hard disk password	Password is set
Screen Saver ✓	Set a password protected keyboard/screen lock. Inactivity period should be no more than 30 minutes.	Account: 7MC9AJFIG1O\Bignon Screen Saver is active: yes Screen Saver is password protected: yes Inactivity period: 26 minutes
Norton AntiVirus ✓	Install and run an approved AntiVirus program. Run Norton AntiVirus LiveUpdate at least weekly.	Version of installed AntiVirus: 7.61.937 AntiVirus running: yes LiveUpdate period: daily
Personal Firewall ✓	Install and run an approved personal firewall program on your workstation if you directly connect the workstation to any customer network, or to the internet via DSL or cable modem, or to any external wireless LAN	Version of installed Firewall: ZoneLabs Firewall 3.5.175.087 Firewall service running: yes Firewall active: yes This data is for your information. It is your responsibility to install and run an . approved personal firewall program if your workstation is connected as described in the **Required result** column.

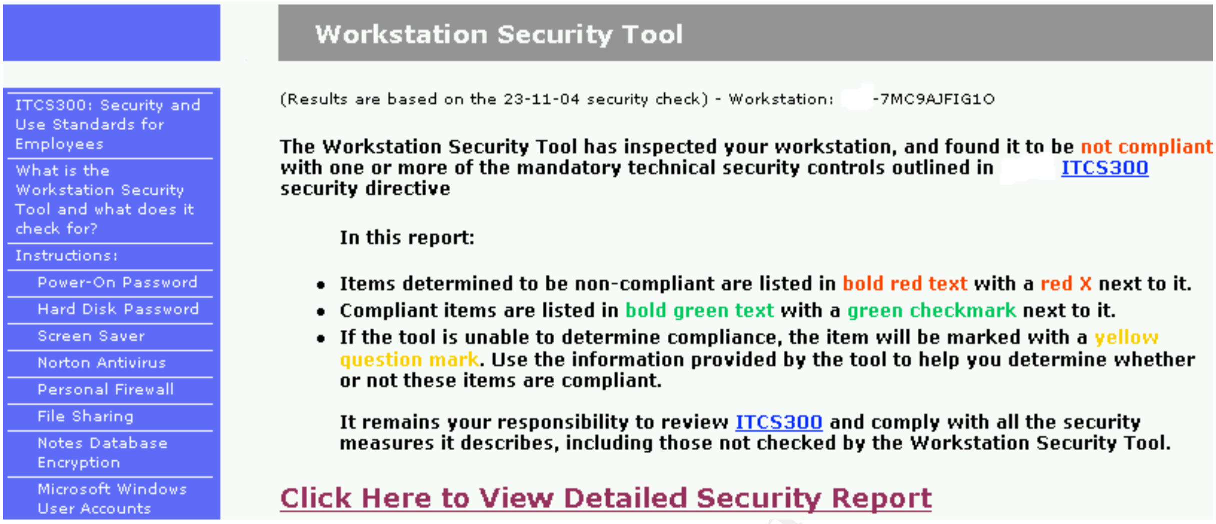


Congratulations! ✓

The Workstation Security Tool is about to update your workstations ITCS300 compliance record.

This data is used to communicate ITCS300 compliance status to you and your manager. To continue and upload your compliance record, click Update. Otherwise, click Exit and your compliance record will be updated at a later date.

Example of Non-Compliant Workstation



- ITCS300: Security and Use Standards for Employees
- What is the Workstation Security Tool and what does it check for?
- Instructions:
  - Power-On Password
  - Hard Disk Password
  - Screen Saver
  - Norton Antivirus
  - Personal Firewall
  - File Sharing
  - Notes Database Encryption
  - Microsoft Windows User Accounts

Workstation Security Tool

(Results are based on the 23-11-04 security check) - Workstation: -7MC9AJFIG1O

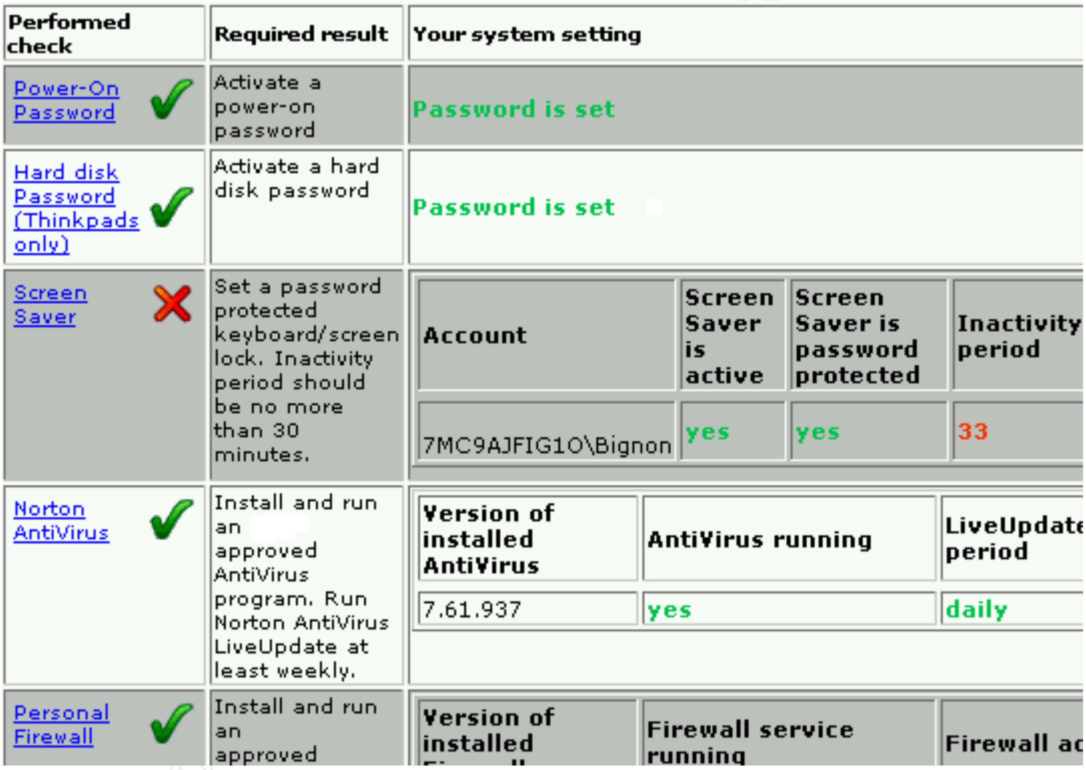
The Workstation Security Tool has inspected your workstation, and found it to be not compliant with one or more of the mandatory technical security controls outlined in ITCS300 security directive

In this report:

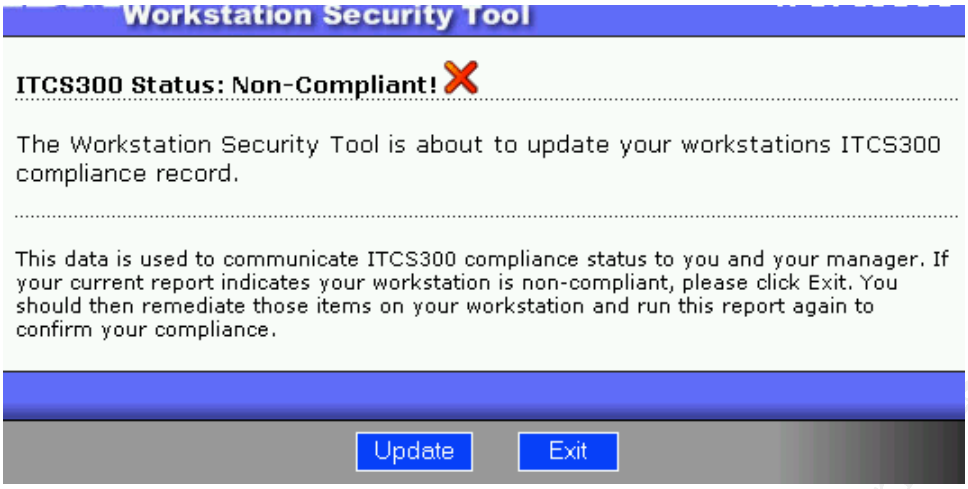
- **Items determined to be non-compliant are listed in bold red text with a red X next to it.**
- **Compliant items are listed in bold green text with a green checkmark next to it.**
- **If the tool is unable to determine compliance, the item will be marked with a yellow question mark. Use the information provided by the tool to help you determine whether or not these items are compliant.**

It remains your responsibility to review ITCS300 and comply with all the security measures it describes, including those not checked by the Workstation Security Tool.

Click Here to View Detailed Security Report



Performed check	**Required result**	**Your system setting**
Power-On Password ✓	Activate a power-on password	**Password is set**
Hard disk Password (Thinkpads only) ✓	Activate a hard disk password	**Password is set**
Screen Saver ✗	Set a password protected keyboard/screen lock. Inactivity period should be no more than 30 minutes.	**Account** | **Screen Saver is active** | **Screen Saver is password protected** | **Inactivity period** 7MC9AJFIG1O\Bignon | **yes** | **yes** | **33**
Norton AntiVirus ✓	Install and run an approved AntiVirus program. Run Norton AntiVirus LiveUpdate at least weekly.	**Version of installed AntiVirus** | **AntiVirus running** | **LiveUpdate period** 7.61.937 | **yes** | **daily**
Personal Firewall ✓	Install and run an approved	**Version of installed** | **Firewall service running** | **Firewall ac**



Workstation Security Tool

ITCS300 Status: Non-Compliant! ✗

The Workstation Security Tool is about to update your workstations ITCS300 compliance record.

This data is used to communicate ITCS300 compliance status to you and your manager. If your current report indicates your workstation is non-compliant, please click Exit. You should then remediate those items on your workstation and run this report again to confirm your compliance.

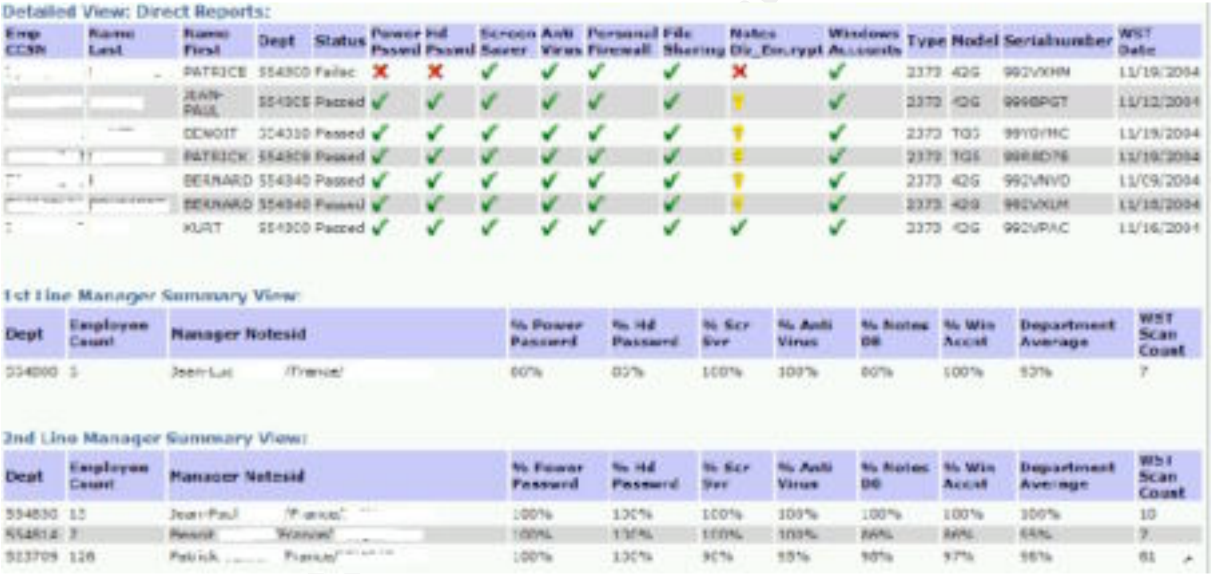
So, in this case the employee must take action immediately to resolve this issue
And rerun WST.

For managers with their staff

Managers have access to:
(via the WAC – WAM Asset Center)

- -The report of his/her direct employees
- -The percentage of compliance of his/her department
- - The percentage of compliance of his/her 2nd line manager
  (depending on the hierarchic order)

Manager Views of WST Data



Detailed View: Direct Reports:

Emp CCSN	Name Last	Name First	Dept	Status	Power Psswd	Hd Psswd	Screen Saver	Anti Virus	Personal Firewall	File Sharing	Notes Dir_Encrypt	Windows Accounts	Type	Model	Serialnumber	WST Date
		PATRICE	554300	Failed	✗	✗	✓	✓	✓	✓	✗	✓	2373	42G	992VXHM	11/19/2004
		JEAN-PAUL	554308	Passed	✓	✓	✓	✓	✓	✓	!	✓	2373	42G	9998PGT	11/12/2004
		BENOIT	554310	Passed	✓	✓	✓	✓	✓	✓	!	✓	2373	TG3	99Y0YMC	11/19/2004
		PATRICK	554808	Passed	✓	✓	✓	✓	✓	✓	!	✓	2373	TG5	998BD76	11/19/2004
		BERNARD	554340	Passed	✓	✓	✓	✓	✓	✓	!	✓	2373	42G	992VNVD	11/09/2004
		BERNARD	554340	Passed	✓	✓	✓	✓	✓	✓	!	✓	2373	42G	992VXLM	11/18/2004
		KURT	554300	Passed	✓	✓	✓	✓	✓	✓	✓	✓	2373	42G	992VPAC	11/16/2004

1st Line Manager Summary View:

Dept	Employee Count	Manager Notesid	% Power Password	% Hd Password	% Scr Svr	% Anti Virus	% Notes DB	% Win Accnt	Department Average	WST Scan Count
554000	1	Jean-Luc /France/	80%	83%	100%	100%	80%	100%	93%	7

2nd Line Manager Summary View:

Dept	Employee Count	Manager Notesid	% Power Password	% Hd Password	% Scr Svr	% Anti Virus	% Notes DB	% Win Accnt	Department Average	WST Scan Count
554830	13	Jean-Paul /France/	100%	100%	100%	100%	100%	100%	100%	10
554814	7	Benoit /France/	100%	100%	100%	100%	86%	86%	95%	7
523709	128	Patrick /France/	100%	100%	90%	95%	98%	97%	98%	81

Fig: View of the manager report

Responsibilities:

Manager's security responsibilities
(in this framework)

- Ensure that employees know, understand, and comply with the Corporate Security Guidelines
- Ensure that these employees ' workstations are compliance by using the WAM Reporting Web Site
- Send to the Business Unit's IT Security dpt a quarterly report (Managers Views of WST data)
- Forbidden any connection in case of 'non-compliance'
- Ensure that employees in their area of responsibility have access only to information based on the rule of "need to know"

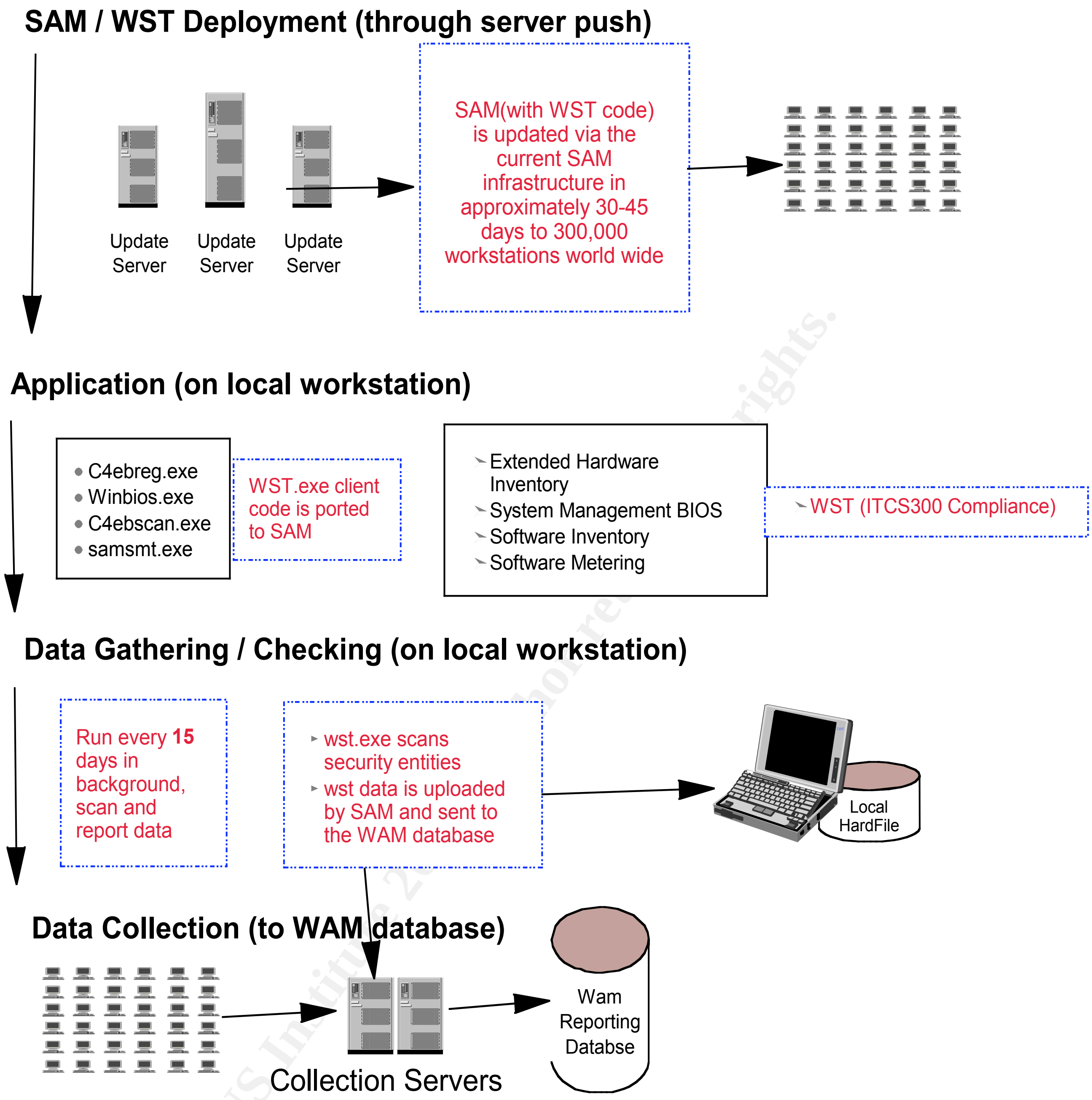
Employee's security responsibilities
(in this framework)

- Knows, understands and complies with the Corporate Security Guidelines
- Ensures that his/her workstation(s) is (are) compliance
- Any derogation will be allowed in case of 'non-compliance'

Measures

- All reports are stored in a database
- A quarterly report is sent to the management

(compliance of the Business Unit)



SAM(with WST code) is updated via the current SAM infrastructure in approximately 30-45 days to 300,000 workstations world wide

WST.exe client code is ported to SAM

Run every **15** days in background, scan and report data

- wst.exe scans security entities
- wst data is uploaded by SAM and sent to the WAM database

Fig-C: SAM / WST Software component and flow

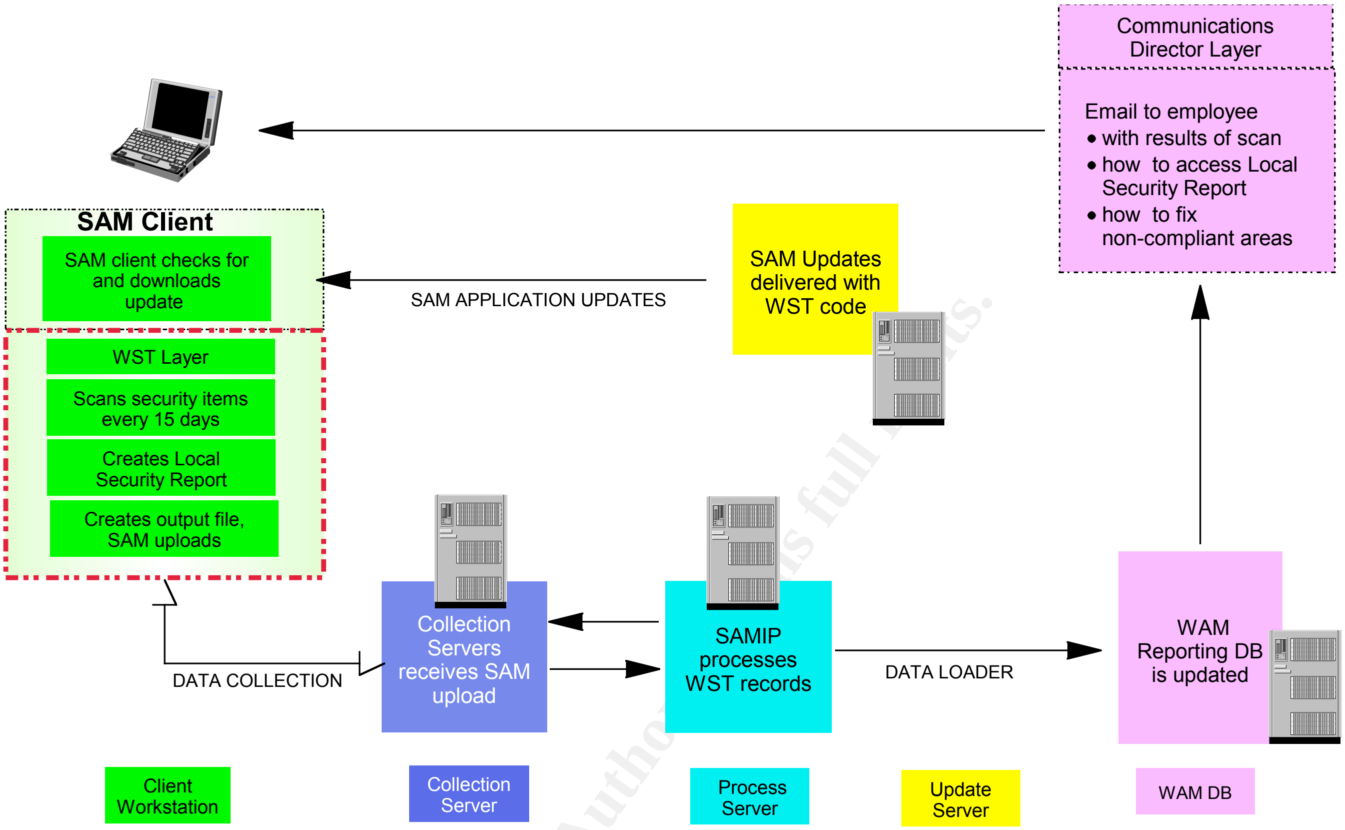

Communications Director Layer
Email to employee
• with results of scan
• how to access Local Security Report
• how to fix non-compliant areas
SAM Client
SAM client checks for and downloads update
SAM APPLICATION UPDATES
SAM Updates delivered with WST code
WST Layer
Scans security items every 15 days
Creates Local Security Report
Creates output file, SAM uploads
Collection Servers receives SAM upload
SAMIP processes WST records
DATA COLLECTION
DATA LOADER
WAM Reporting DB is updated
Client Workstation
Collection Server
Process Server
Update Server
WAM DB

Fig-D: SAM / WST Infrastructure Diagram

Automated Security Patching

My company introduces a patch management solution to automatically deliver patches for workstation vulnerabilities while employees work.

EZUpdate (its name) is a small agent that runs on the employee's workstations.

Maintaining a computer environment secure from attacks of vulnerabilities found in Microsoft applications and operating systems is a paramount concern for company.
At the same time, asking employees to keep up with new security patches has proven frustrating, boring and confusing.
Ant it was strictly forbidden downloading patches from the Microsoft web Site onto company's workstations. Employees had to wait for patches are customized, tested in our environment and available in SSI, so as not to cause conflict with other security measures already in place.

Everyone has called for an automated like WST.

Company has begun rolling out a new process to deliver security patches to individual employee s' workstations automatically in the background by way of an upgraded EZUpdate, the companion to Standards Software Installer. This automated solution takes the guesswork out of the security patch management so our workstation is always current.

Here is how EZUpdate patch delivery works:

- It wakes up daily to check if there are any critical security fixes to be delivered to the workstation from SSI. When a critical fix is needed the tool automatically downloads it from SSI, notify us that it has done so and will immediately begin installing the patch. We may have to re-boot our computer during the process, EZUpdate will automatically do so after eight hours.
- EZUpdate automatically engages Standard Asset Manager (SAM), so that it can report that we have the current security fixes installed.

To ensure that company maintains a secure and sound computing infrastructure it's the manager's responsibility to ensure that EZUpdate (the SSI client side companion agent), is installed on all employee's Windows workstations.
An automatic control by WST verifying that EZUpade is active on workstations is coming very soon.

How about virus notes?

There is good news to report. Company has begun deleting all those e-mails that have been scrubbed of worm or virus attachments before they reach our inbox. We have already seen a lot less junk in our e-mail.
This doesn't mean worms and virus will not get through anymore. It simply means those are identified as containing a worm or virus will be deleted.
(Rule: Never open suspicious or unexpected e-mail attachments.)

Password compliance Tool

This password policy update tool will modify the security parameters of our Windows XP/2000 workstations into compliance with our Corporate Security Guidelines password requirement.
Under these requirements, passwords must be at least 8 positions in length and must be expire after 90 days.
Beginning in Q2-2005, the Workstation Security Tool will begin validation compliance to the password requirement for all workstations.

Conclusion

In an ideal world, we could all forget about IT Security, be confident our data is protected, and know our system were safe from viruses, worms and other hostile network nuisances.
Of course our IT world is not ideal
Security is neither easy nor intuitive and security is a never ending process.
But it remains a collaborative and vital effort among the IT-Teams working with individual employees to keep their workstations up to date with software patches, anti-virus protection, personal firewalls, etc….
The challenge of the Company is to simplify security process for employees, even automate them to the point of transparency.
By focusing on further automating our security tools, we hope to make it easier for everyone to do their part.

References

-My company's intranet
-SANS Institute:
Defense-In-Depth (Book 1 p64-65 / Book 2 p94)
Secure Communication (Book 4 p250-257-259)
Windows Security (Book 5 p185)
http://www.alw.nih.gov/Security/security.html
http://www.infopeople.org/resources/security/workstation/about.html
http://www.ae-solutions.com/workstationsecurity.php
http://infosec.bsd.uchicago.edu/policies/workstation_security.html
http://www.gla.ac.uk:443/cert/prevention/guides/index.shtml

**** End of Document ****